End of Result Set

Generate Collection | Print

L2: Entry 8 of 8 File: USPT Nov 24, 1981

US-PAT-NO: 4302810
DOCUMENT-IDENTIFIER: US 4302810 A

TITLE: Method and apparatus for secure message transmission for use in electronic funds transfer systems

DATE-ISSUED: November 24, 1981

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Bouricius; Willard G.	Katonah	NY		
Stuckert; Paul E.	Katonah	NY		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 06/ 108071 [PALM]
DATE FILED: December 28, 1979

INT-CL: [03] G06F 3/023, G06F 7/04, G06F 15/02, G06F 15/30

US-CL-ISSUED: 364/200
US-CL-CURRENT: 705/75; 380/37, 380/45, 705/73, 705/78, 902/2, 902/22

FIELD-OF-SEARCH: 235/379-381, 340/149A, 364/2MSFile, 364/9MSFile

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3544769	December 1970	Hedin	235/379
☐	3636520	January 1972	Berteau	364/200
☐	3852571	December 1974	Hall et al.	235/379
☐	4183085	January 1980	Roberts et al.	364/200
☐	4198619	April 1980	Atalla	235/381

ART-UNIT: 237

PRIMARY-EXAMINER: Springborn; Harvey E.

ATTY-AGENT-FIRM: Schlemmer, Jr.; Roy R.

ABSTRACT:

An electronic funds transfer system wherein it is required that a bank be reasonably guaranteed that the two parties to a retail transaction (i.e., a person and a retailer) agree on the transaction before the funds transfer takes place. The message including the transaction information is encrypted by the person using a unique encryption key (K.sub.P) stored in a highly secure storage location in his own personal portable transaction device (XATR) and his data storage and transfer card (DSTC) and this first encrypted message is sent to the retailer who doubly encrypts the initially received encrypted message from P under his own unique encryption key (K.sub.R) and this doubly encrypted message is sent to the bank. The person also sends the transaction message to the retailer in clear, and the retailer first verifies the message and then, utilizing his own encryption key (K.sub.R), encrypts same and similarly sends it to the bank. The bank utilizing unique retailer and customer identification data sent with the message, accesses a "key" file and first extracts the retailer's key (K.sub.R) and decrypts a first portion of the message, extracts the person's key (K.sub.P) and decrypts a second portion of the received message. The bank then compares a predetermined portion of the transaction message originating with the person with a similar portion received from the retailer and if identical, the appropriate funds transfer is made. If the messages do not agree, a predetermined default procedure is initiated.

12 Claims, 7 Drawing figures